VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

PŘÍSTUPOVÝ SYSTÉM VYUŽÍVAJÍCÍ NFC A MIKROPOČÍTAČE ARDUINO
ACCESS CONTROL SYSTEM UTILIZING NFC AND ARDUINO MICROCONTROLLER

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jaroslav Hájek**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Jiří Hošek, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Jaroslav Hájek ***ID:*** 173649
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Přístupový systém využívající NFC a mikropočítače Arduino

POKYNY PRO VYPRACOVÁNÍ:

Mezi dnes nejpoužívanější přístupové systémy se řadí systémy s autentizací uživatelů pomocí předmětů (zejména NFC tokeny). S masivním rozšířením chytrých mobilních zařízení podporující technologii NFC a HCE (Host-based Card Emulation) lze těchto zařízení využít jako autentizačních předmětů. Bakalářská práce se proto bude zabývat návrhem přístupového systému s autentizací uživatelů pomocí předmětů. Přístupový systém bude založen na vývojových platformách Arduino a Raspberry PI, které budou komunikovat skrze technologii Wi-Fi. Jako autentizační předmět bude sloužit moilní telefon s technologií NFC. Součástí výsledků práce bude vlastní aplikace pro operační systém Android využívající implementace technologie HCE. Implementace bude zahrnovat také vývoj uživatelského rozhraní s databází umožňující vizualizaci přístupů do systému.

DOPORUČENÁ LITERATURA:

[1] MARGOLIS, Michael. Arduino Cookbook. 2. Sebastopol: O'REILLY, 2012. ISBN 978-1-449-31387.

[2] IGOE, Tom., Don. COLEMAN a Brian. JEPSON. Beginning NFC: near field communication with Arduino, Android, and Phonegap. Beijing: O'Reilly, 2014. ISBN 14-493-7206-6.

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 8.6.2017

Vedoucí práce: doc. Ing. Jiří Hošek, Ph.D.
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce se zabývá přístupovými systémy včetně administrace zámků, skupin uživatelů, uživatelů a jejich identit. Vytvořený systém se sestává z čtyř hlavních bloků, kterými jsou: webové rozhraní Locker, serverová aplikace Authentizer, MySQL databáze a Android aplikace. Webové rozhraní slouží pro administraci systému a komunikuje s databází. Serverová aplikace zajišťuje komunikaci zámků s MySQL databází a jejím hlavním úkolem je ověřování identit uživatelů. Serverová aplikace slouží také jako API, které lze využít pro komunikaci s externími aplikacemi. Vytvořená aplikace pro systém Android umožňuje nahrazení přístupového NFC tokenu mobilním telefonem.

KLÍČOVÁ SLOVA

Android, Arduino, Authentizer, I2C, Locker, MySQL, NDEF, NFC, PN532, přístupový systém, Raspberry Pi, RFID, TNF

ABSTRACT

The Bachelor thesis focuses on acces systems including administration of locks, groups of users, users and their identities. For simple implementation of the system have been created four significant elements of the project: a web interface Locker, an application server Authentizer, MySQL database and an Android application. The web interface is used for system administration and included communication with the database. The server application is used for a communitation between the Locks and the MySQL database. The pivotal role of the server application is verification identities of users. The sever application and the database are used as publishing API. Android application is used as identity instead of identity card.

KEYWORDS

Android, Arduino, Authentizer, I2C, Locker, MySQL, NDEF, NFC, PN532, access system, Raspberry Pi, RFID, TNF

HÁJEK, Jaroslav *Přístupový systém využívající NFC a mikropočítače Arduino*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Rok. 54 s. Vedoucí práce byl Ing. Jiří Hošek, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Přístupový systém využívající NFC a mikropočítače Arduino“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Jiřímu Hoškovi, Ph.D., Ing. Martinu Štůskovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Dále bych chtěl poděkovat Dagmar Stromšíkové, Martinu Bednářovi a rodičům za cenné rady a podporu.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Bakalářská práce se zabývá bezdrátovým přístupovým systémem využívající technologii NFC (Near Field Communication). V oblasti velkých podniků či veřejně přístupných prostor vzniká potřeba řídit či kontrolovat přístupy do budov či oblastí. K tomuto účelu se používají přístupové systémy, jejichž úkolem je autentizace uživatelů. Tato bakalářská práce se zabývá systémy využívající tzv. autentizaci pomocí předmětů. Uživatel je v tomto případě autentizován na základě vlastnictví předmětu. Jako komunikační rozhraní předmětů a čtečky slouží technologie NFC. Vytvořená platforma se skládá z čtečky NFC tagů připojené k mikrokontroléru Atmega 328p, která komunikuje s aplikací na straně serveru skrze technologii WiFi. Jako čtečka NFC tagů slouží vývojový modul PN532, tento model byl vybrán z důvodu podpory protokolů simulace karet HCE (Host Card Emulation) na platformě Android. Pro komunikaci WiFi je použit modul založený na čipu ESP8266, který je nejvhodnější variantou pro platformu Arduino z důvodu vysoké spolehlivosti a nízké ceny. Serverová aplikace autentizuje uživatele na základě přiložených karet a zařízení s technologií HCE oproti databázi. Pro uživatelsky přívětivé ovládání je vytvořeno grafické webové rozhraní umožňující snadnou správu (přidání, mazání, editaci) uživatelských účtů, ale také přístupových zámků. Každý přístup do systému je rovněž ukládán do databáze a je přehledně zobrazen v uživatelském rozhraní. Správce systému má proto přehled o jednotlivých přístupech do systému, navíc také na první pohled rozezná přidělení či odmítnutí přístupu uživateli, jelikož jsou jednotlivé události rozlišeny barevně dle stupně důležitosti.

1 PŘÍSTUPOVÉ SYSTÉMY

Moderní přístupové systémy se zaměřují na autentizaci uživatelů pomocí předmětů, které regulují oprávnění vstupu do prostor nepřístupných osobám nepovolaným. Prostory lze rozdělit na reálné a virtuální. Mezi virtuální prostory patří např. elektronické, komunikační nebo informační systémy. Mezi reálné jsou řazeny místnosti či budovy. Žadatelé se při pokusu o oprávnění prokazují svým identifikátorem. Systém podle identifikátoru určí přístupová práva žadateli a na jejich základě otevře dveře či zábrany. Tato místa jsou nazývány přístupové body. Mezi hlavní výhody patří například kontrola nad přístupem uživatele. Můžeme tedy kontrolovat, kam uživatel přístup má a kam nikoliv. Další důležitá výhoda je při odcizení karty uživateli. V této situaci ji může administrátor ze systému vymazat a tím zamítnout přístup do objektu[1].

1.1 Typy přístupových systémů

Přístupové systémy lze dělit podle množství uživatelů, důležitosti zabezpečení, nebo celkové administrativy. Hlavní skupiny přístupových systému jsou popsány v následujících sekcích.

1.1.1 Autonomní systémy

Autonomní systémy fungují na zákldě administratorských karet (Master Card). Tyto karty slouží ke změně, přídání nebo odebrání přístupových práv kartě jiné. U těchto systémů odpadá nutnost mít přípojený jiný ověřovací či administrativní prvek [8].

1.1.2 Systém skupin

Systém skupin dokáže definovat oprávnění skupiny uživatelů. Tento systém je vhodný k použití ve firmách, nebo školách. Zde můžeme definovat skupinu žáci a školní vedení. Skupina žáci bude mít například oprávnění vstupu do studovny [10].

1.2 Monitoring

Každé povolení, nebo zakázání vstupu by mělo být monitorované. Monitoring je velice důležitý, protože zjišťuje neoprávněné vstupy. Obvykle bývá zajištěn logem, do kterého jsou zapsány časy povolených či zamítnutých vstupů do prostor. Druhá varianta je použití kamer, které ukládají záznam s přesným časem [9].

2 TECHNOLOGIE NFC

Tato technologie umožňuje bezdrátovou komunikaci typu bod-bod na krátkou vzdálenost mezi dvěma zařízeními. Technologie NFC byla původně vytvořena pro platební transakce. Časem ji společnost Google za pomocí mobilního operačního systému Android (implementovanou ve verzi 2.3 (Gingerbread)) rozšířila i do dalších odvětví moderních technologií např. párování zařízení po přiložení či nastavení WiFi po kontaktu s NFC tagem [11].

2.1 RFID (Radio Frequency Identification)

Jedná se o technologii přímo předcházející modernějšímu NFC využívanou u bezkontaktních karet nebo čipů. Pro komunikaci může využívat nosnou frekvenci 125 kHz, 134 kHz a 13,56 MHz. Díky malému vysílacímu výkonu je potřeba kartu přiložit jen pár centimetrů od přijímacího zařízení, aby mezi sebou zařízení komunikovala. Lze rozlišit dva typy tagů, aktivní a pasivní. Aktivní jsou napájeny baterií a vysílají data nezávisle na čtečce. Pasívní obsahují kondenzátor, který se nabíjí přes komunikační anténu a data odesílá pouze po přiložení ke čtečce [12].

2.2 NFC režimy kominukace

Technologie NFC definuje 3 základní režimy komunikace a to

- čtení a zápis,
- peer to peer,
- card emulation.

2.2.1 Režim čtení a zápisu

Tento režim je zvolen, pokud jsou k sobě přiloženy aktivní a pasivní prvek například čtečka karet a NFC tag. Během této komunikace lze z karty číst, nebo na ní zapisovat. Aktivní prvek se nazývá iniciátor. K této komunikaci jsou použity tzv. NDEF (NFC Data Exchange Format) zprávy popsané v kapitole 2.5 [5].

2.2.2 Režim Peer to Peer

V tomto režimu spolu komunikují dva aktivní prvky (oba jsou tedy napájeny vlastním zdrojem) a slouží ke komunikaci v obou směrech. Tato komunikace je typu half-duplex a rychlost komunikace dosahuje až 424 kbit/s. NFC fórum definovalo protokol LLCP (Logical Link Control Protocol), který odpovídá spojové vrstvě modelu

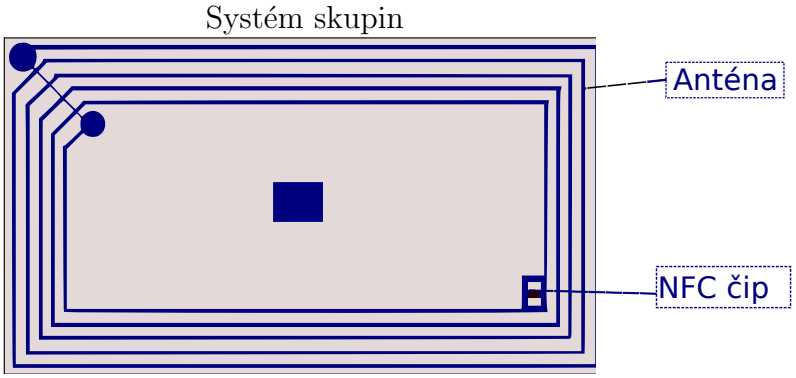
OSI (Open Interconnection Reference). Protokol LLCP zajišťuje aktivaci sledování a odpojení při spojované i nespojované komunikaci [5].

2.2.3 Režim card emulation

Tento režim byl vytvořen pro aktivní zařízení k tomu, aby simulovali pasivní NFC tagy. Pokud je zařízení nastaveno v tomto režimu, komunikaci inicializuje čtečka a mobilní zařízení je vnímáno jako NFC tag. Do verze Androidu 4.4 (KitKat) šlo použít režim emulace karty jen za pomocí bezpečnostního prvku (Secure Elementu), který byl většinou umístěn v SIM (Subscriber Identify Module) kartě. Secure Element je integrovaný čip v SIM kartě, nebo SD (Secure Digital) a obsahuje paměť a zabezpečený koprocsesor. Funguje tak, že je do něj přenesena aplikace a s NFC rozhráním komunikuje pouze Secure Element. Od verze Androidu 4.4 je komunikace možná i bez Secure Elementu s NFC rozhraním, v tomto případě komunikuje aplikace přímo [5].

2.3 NFC Tag

NFC tag je pasivní čip, to znamená, že k jeho fungování není zapotřebí napájení ve formě baterie. Jeho napájení zajišťuje aktivní prvek, ke kterému je přiložen.
K přenesení energie je použita elektromagnetická indukce, ta skrze anténu (která v tagu zabírá nejvíce místa) nabíjí kondenzátor. NFC tag dále obsahuje řídící jednotku a paměť. Schéma pasivního NFC tagu je uvedeno na Obr. 2.3.



Obr. 2.1: Schéma pasivního NFC tagu.

2.4 Typy NFC tagů

Technologie NFC definuje čtyři různé typy NFC tagů, které jsou uvedeny v tabulce Tab. 2.1 [6].

Tab. 2.1: Typy Tagů.

TYP	**1**	**2**	**3**	**4**
NORMA	ISO/IEC 14443	ISO/IEC 14443	FeliCa	ISO/IEC 14443
ČTENÍ	ANO	ANO	ANO	ANO
ZÁPIS	ANO	ANO	Při výrobě	Při výrobě
KAPACITA	96 B - 2048 kB	48 B - 2048 kB	0 B - 1 MB	0 B - 32 kB
RYCHLOST	106 kb/s	106 kb/s	212 kb/s (424 kb/s)	106 kb/s (424 kb/s)

2.5 NDEF (NFC Data Exchange Format)

NFC fórem byl vytvořen datový formát NDEF. Tento datový formát standardizuje komunikaci mezi NFC tagy a čtečkami. Díky tomuto standardu je ušetřena kapacita karty. Pokud jsou například do tagu uloženy kontaktní údaje a později je přiložen k mobilnímu zařízení, po přečtení zobrazí data z tagu jako vizitku. Pokud je přiložen tag s URL (Uniform Resource Locator), otevře se prohlížeč s načteným URL. NDEF formát je připraven také na obrazová data, či konfigurace připojení k síti, nebo inicializace připojení k bluetooth zařízení například bezdrátové reproduktory. Po přiložení mobilního zařízení je umožněno připojení k bluetooth zařízení a je možné okamžité přehrávání, bez párovaní mezi zařízeními. Rozložení formátu NDEF je popsáno v Tab. 2.2.

NDEF zpráva může obsahovat jeden, nebo více NDEF záznamů.
První záznam obsahuje příznak MB (Message Begin). Poslední záznam obsahuje příznak ME (Message End). Pokud zpráva obsahuje pouze jeden záznam, je opatřen příznaky MB i ME. Každý záznam je očíslován. Jeho index je v příznaku MB. Pokud je odeslán poslední záznam příznak MB má hodnotu n a příznak ME má hodnotu 1.

- **SR (Short Record)**: příznak SR je jednobitový příznak rozlišující jestli jde o zprávu běžnou SR=0, nebo krátkou SR=1, pokud jde o zprávu krátkou, je použit jeden oktet na místo čtyř,
- **IL (ID Length)**: pokud je jednobitový příznak IL roven 1, jsou pole ID a ID LENGHT přítomny v NDEF záznamu a každý zabírá jeden oktet, pokud je IL roven 0 tak jsou vynechány,

Tab. 2.2: NDEF Formát.

7	6	5	4	3	2	1	0
MB	ME	CF	SR	IL	TNF		
TYPE LENGTH							
PAYLOAD LENGTH 3							
PAYLOAD LENGTH 2							
PAYLOAD LENGTH 1							
PAYLOAD LENGTH 0							
ID LENGTH							
TYPE							
ID							
PAYLOAD							

- **TNF (Type Name Format)** : je tříbitový příznak určující typ přenášených dat. Tento příznak je popsán v Tab. 2.3[7].

Tab. 2.3: TNF (Type Name Format).

Příznak	Název záznamu	Popis
0x00	Empty Record	Je vhodný pro nově vyrobené karty. Nemá definovaný typ, ID nebo PayLoad.
0x01	Well-Known Record	Obsahuje typ definovaný podle NFC Fóra. Tento typ je uložen v položce TYPE. Jsou zde nejčastěji používané typy jako je URI nebo TEXT.
0x02	Media Record	Přenáší typ média podle standardu RFC 2046 [15].
0x03	Absolute URI Record	Obsahuje záznam absolutní URI specifikovaný dle RFC 3986 [16].
0x04	External Record	Externí typ NFC Fóra (pole Type obsahuje jméno ze specifikace NFC RTD.
0x05	Unknown Record	Označuje neznámý typ dat.
0x06	Unchanged Record	Nezměněný záznam.

2.6 Norma bezdrátové komunikace na krátkou vzdálenost ISO/IEC 14443

Tento komunikační standard definuje bezdrátovou komunikaci na krátkou vzdálenost pracující se střední hodnotou nosné frekvence 13,56 MHz. Norma definuje elementy PICC (Proximity Integrated Circuit Card) a PCD (Proximity Coupling Device). Jako zdroj napájení slouží čtečka, která vytváří elektromagnetické pole napájející přiložená pasivně napájená komunikační zařízení. Elektromagnetické pole slouží i jako přenašeč dat a to tak že přerušuje tok magnetické indukce v krátkých časových interval. Interval přerušení magnetického pole je tak krátký aby nezpůsobil restart karty. Začátek komunikace je definován prvním přerušením elektromagnetického pole. Následuje přenos dat a poté ukončení komunikace [17].

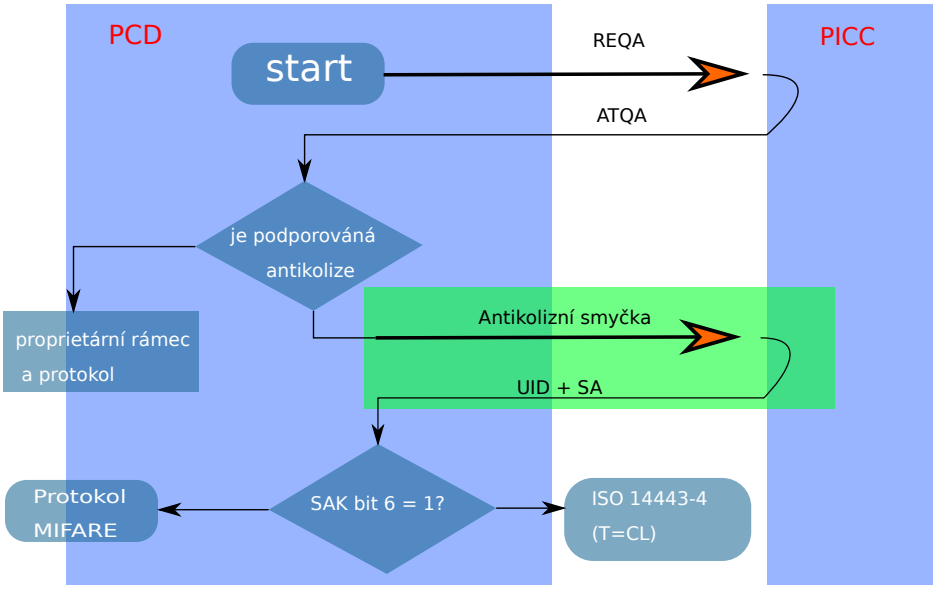
2.6.1 Podsekce normy ISO/IEC 14443

Norma je rozdělena na čtyři části.

- ISO/IEC 14443-1 - První část normy se zabývá fyzickou částí karet a to především jejich velikostí ohebností nebo odolností vůči rentgenovému či ultrafialovému záření. Tato sekce definuje také elektromagnetické podmínky, ve kterých lze karty provozovat.
- ISO/IEC 14443-2 - Druhá část popisuje přenosové frekvence, které jsou při komunikaci použity. Obsahuje také podrobný popis časování u signálů v protokolu.
- ISO/IEC 14443-3 - Ve třetí části norma popisuje inicializační a antikolizní protokoly k oběma typům PICC (pro aktivní i pasivní v obou směrech komunikace). Dále určuje stavy karty a kódování příkazů i odpovědí.
- ISO/IEC 14443-4 - Čtvrtá a poslední část normy popisuje navázání komunikace s kartou pro vysokoúrovňový přenos dat.

2.6.2 Inicializace Karty

Komunikace probíhá v modelu Master (čtečka) a Slave (karta). Čtečka stále vysílá nosnou frekvenci s periodicky se opakujícím příkazem REQ (Request Command,Type A). Pokud je tedy karta umístěna do elektromagnetického pole čtečky odpoví svým ATQA (Answer To Request, Type A). Další komunikace už probíhá vždy jako odpověď karty na požadavek čtečky. Probíhá zde také antikolizní smyčka. Ta slouží k tomu, aby se čtecí zařízení a transpondér dohodli na jediném komunikačním páru čtečka - transpondér, pokud je v dosahu čtecího zařízení víc než jedno zařízení. Životní cyklus inicializačního řetězce s antikolizní smyčkou je uveden na obrázku 2.2.



Obr. 2.2: Inicializace Karty.

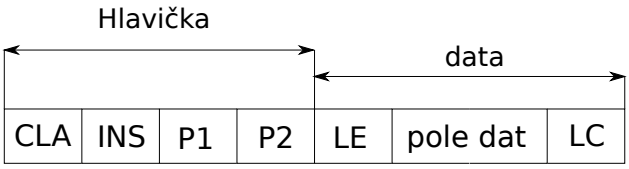
2.7 Norma ISO/IEC 7816-4

Tato norma popisuje jednotku APDU (Application Processing Data Unit). Tyto protokoly slouží k výměně datových struktur.

APDU má dvě formy a to

- Příkaz APDU - je odesílán za čtečky na kartu,
- Odpověď APDU - je odesílán za karty na čtečku.

Příkaz APDU je rozdělen na hlavičku a tělo. Jak je znázorněno na obrázku Obr. 2.3



Obr. 2.3: Struktůra APDU.

- CLA - Třída Aplikace,
- INS - Instrukce,
- P1, P2 - Parametry instrukce.

Tělo APDU zprávy může mít různou velikost a je odesláno do APDU procesoru karty. LC určuje počet bajtů, které jsou předávány na kartu jako část instrukcí,

ty jsou nazvány datové pole. Toto datové pole obsahuje informace, které musí být odeslány do APDU processoru karty pro vykonání APDU příkazu. LE určuje počet bajtů, které budou vráceny z karty do čtecího zařízení. APDU zpráva může nabývat těchto čtyřech forem:

- 1 - APDU obsahuje pouze hlavičku, žádná data nejsou poslána kartě a žádná data nejsou po kartě požadována.
- 2 - APDU obsahuje hlavičku a v těle je pouze pole LE. To znamená, že žádná data nejsou kartě odeslána, ale očekává se příjem dat od karty.
- 3 - APDU obsahuje hlavičku a v těle je pole LC a pole dat. Kartě odeslána data, ale už se neočekává příjem dat z karty.
- 4 - APDU obsahuje hlavičku a v těle jsou pole LC, LE a pole dat. To znamená, že jsou kartě odeslána data a je očekáván i příjem dat z karty.

Struktura APDU odpovědí je jednodušší než u APDU příkazů. Protože jejich odpověď se skládá z těla a statusu. Tělo může být prázdné nebo zahrnuje pole dat. To záleží na konkrétním příkazu. Délka datového pole je určená hodnotou LE příkazového APDU. Status je tvořen dvěma poli SW1 a SW2, které vrací informace o stavu odpovědi. Tato pole vracejí stavový kód, kde jeden bajt určuje kategorii chyby a druhý označuje údaj o chybě. Mnoho zařízení používající operační systém Android a vlastnící funkci NFC podporuje také možnost emulace hostované karty. V mnoha případech je karta emulována odděleným čipem nazýván jako secure element (bezpečnostní prvek). Mnoho SIM karet dodávaných operátory také obsahuje tento bezpečnostní prvek. Od verze systému Android 4.4 již není zapotřebí bezpečnostní prvek ale karta komunikuje přímo s aplikací [18].

3 POUŽITÝ HARDWARE

Mezi hardware použitý v této bakalářské práci patří:

- Arduino,
- Raspberry PI 3,
- ESP 8266,
- PN532.

3.1 Arduino

Platforma Arduino je rodinou jednodeskových mikropočítačů založených téměř výhradně na 8-bitových mikrokontrolerech firmy Atmel. Celý projekt je šířen pod licencí open source, a proto existuje velké množství připravených knihoven či rozšifrujících modulů (shields). Analogové vstupy jsou připojeny na šestikanálový, desetibitový A/D převodník. Ten je součástí Arduina a jeho vstupy jsou připojeny na piny A0–A5. Arduino také obsahuje FTDI (Future Technology Devices International) čip, který zajišťuje konverzi UART (Universal Asynchronous Receiver/Transmitter) rozhraní na USB (Universal Serial Bus), které slouží pro komunikaci s PC (Personal Computer)[2]. Funkcionalitu hardware lze rozšiřovat pomocí tzv. Shields, modulů které s Arduinem komunikují skrze sériová rozhraní (UART, SPI, I2C)[14].

3.1.1 Arduino IDE

Arduino IDE (Integrated Development Environment) je software určený k programování vývojových desek Arduino. Program se zapisuje do souborů, které se v názvosloví Arduino nazývají Sketch a jsou ukládány do tzv. Sketchbook. I když je IDE speciálně navrženo pro vývojové desky Arduino, není to podmínkou. Pokud použijeme jeden z mikrokontrolerů obsažených na vývojových deskách Arduino, je možné po vypálení bootloaderu do flash paměti programovat i kompatibilní mikrokontrolery. Tato metoda je vhodná u projektu, kde není žádoucí použít vývojovou desku Arduino. Lze tedy navrhnout vlastní desku obsahující kompatibilní mikroprocesor s vypáleným zavaděčem. Takový mikrokontroler lze programovat stejně jako vývojovou desku Arduino.
Výhodou platformy Arduino je velké množství předpřipravených knihoven, které programátorovi usnadňují vývoj. Základními prvky Aarduino IDE jsou tlačítka pro ověření, nahrání, založení nového souboru, otevření souboru, nebo uložení a tlačítko pro otevření terminálu sériového portu. Tlačítko ověření slouží ke kontrole programu a nalezení chyb, které může program obsahovat. Pokud vývojové prostředí chyby odhalí, nedovolí projekt nahrát do vývojové desky a zabrání nechtěnému zničení desky.

Položka Sériová konzole bývá použita jako jeden z výstupů projektu, ve které lze zobrazovat hodnoty proměnných, výstupů ze senzorů či jiná data.
Ve vývojovém prostředí Arduino je jako primární programovací jazyk zvolen Wiring. Jazyk Wiring však není plnohodnotným programovacím jazykem, ale poskytuje dodatečné funkce nad jazykem C++. Ten slouží jako základ tohoto frameworku. Použití jazyka Wiring však není nutností a lze využít čistou podobu jazyka C++, např. z důvodu rychlosti programu [13].

3.1.2 Struktura programu a knihovny

Programy napsané pro platformu Arduino obsahují dvě základní části:

- setup - tato sekce slouží k nastavení vstupů/výstupů či inicializaci proměněných,
- loop - zde se vykonává samostatný program v nekonečné smyčce.

Program pro blikání led diody může vypadat například takto:

```
1  void setup() {
2    int LED = 13;
3    pinMode(LED,OUTPUT);
4  }
5  void loop() {
6    digitalWrite(LED, HIGH);
7    delay(1000);
8    digitalWrite(LED, LOW);
9    delay(1000);
10 }
```

3.1.3 Arduino zavaděč

Většina desek vývojové platformy Arduino obsahuje processor od firmy Atmel, ve kterém je nahrán zavaděč Arduina. Zavaděč je umístěn na konci flash paměti a slouží pro komunikaci mezi vývojovou deskou a prostředím Arduino IDE. Po připojení napájení k vývojové desce se nejdříve spustí zavaděč [3].

3.1.4 Nejčastěji používané vývojové desky

Nejčastěji se používají tři základní typy vývojových desek Arduino, jejich parametry jsou uvedeny v Tab. 3.1

Tab. 3.1: Základní typy Arduino.

	Arduino Uno	Arduino Nano	Arduino Mega
Procesor	ATmega328P	ATmega328	ATMega2560
Frekvence	16 MHz	16 MHz	16 MHz
Digitální piny	14	14	54
Analogové piny	6	8	16
Napájení	5V (USB) 7-16V (adaptér)	5V (USB) 5V pin na desce	5V (USB) 7-16V (adaptér)
Rozměry	69x53x12 mm	18,5x43 mm	102x53x12 mm
Sběrnice	1x HW UART I2C	SPI I2C	4x HW UART 12C

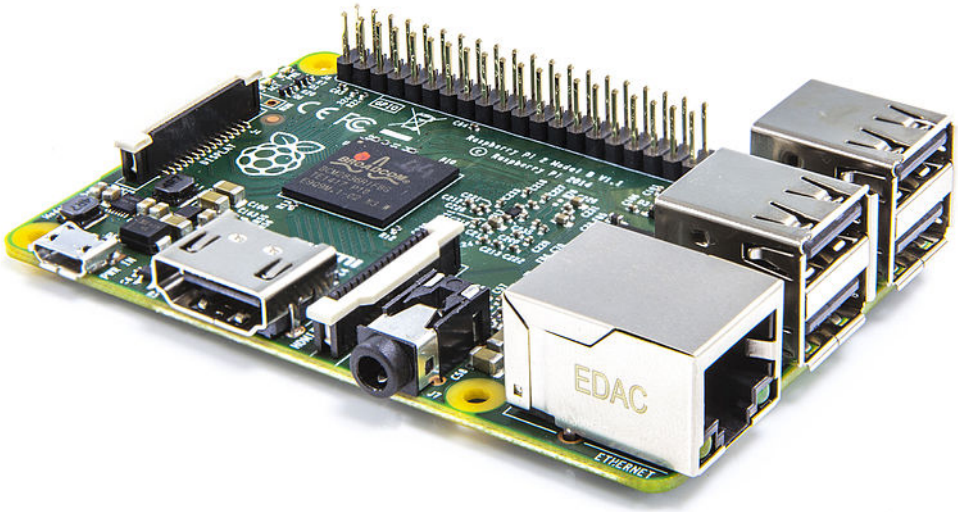
3.2 Raspberry PI 3

Raspberry PI je malý výkonný a programovatelný počítač, který je založen na architektuře ARM (Acorn RISC Machine) jehož parametry jsou uvedeny v Tab. 3.2.

Tab. 3.2: Parametry Raspberry PI.

Procesor (CPU)	1.2GHz 64-bitový čtyřjádrový ARM Cortex-A53
Video (GPU)	Broadcom VideoCore IV @ 400 MHz / 300 MHz, OpenGL ES 2.0 (24 GFLOPS),,MPEG-2 a VC-1 (s licencí), 1080p30 H.264/MPEG-4 AVC dekodér a kodér, s vysokým profilem
Paměť (SDRAM)	1 GB (sdílená s GPU)
Kontektory	15-pinový MIPI konektor kamerového rozhraní (CSI) TRRS Jack 4x USB pro periferie Ethernet MicroUSB (napájení)

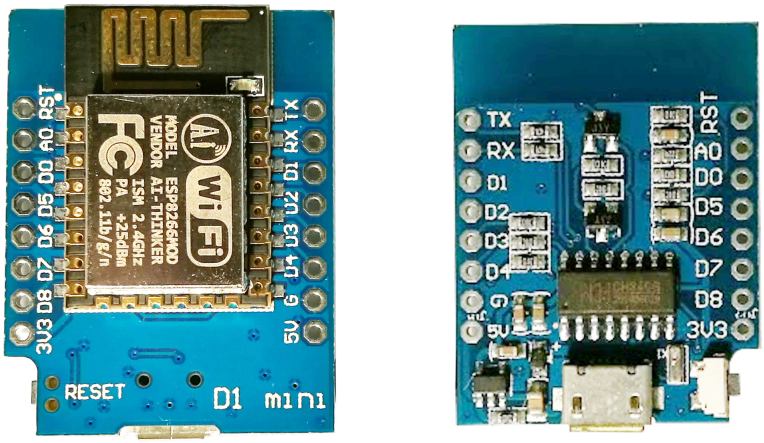
Raspberry PI je použito v bakalářské práci v roli MySQL (My Structured Query Language), Apache serveru a je zde spuštěna serverová aplikace komunikující se zámky. Zařízení dále slouží jako přístupový bod s SSID (Service Set Identifier) „Locker“ na který se zámky připojují.



Obr. 3.1: Raspberry PI 3 [4].

3.3 Wemos D1 mini

Wemos D1 mini je WiFi modul založený na čipu ESP8266, který lze programovat pomocí více jazyků např. Lua, MicroPython, Arduino. V práci byl zvolen scriptovací jazyk Lua, protože je v něm nejlépe vyřešena komunikace prostřednictvím TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). Toto zařízení bylo v práci použito pro bezdrátovou komunikaci s autentizačním serverem.



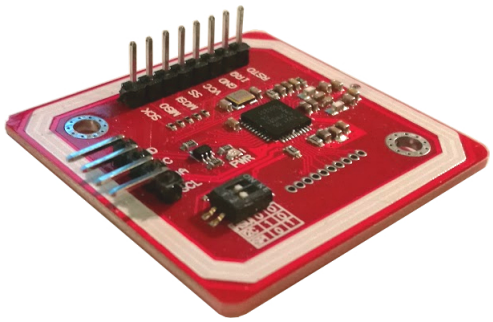
Obr. 3.2: Wemos D1 mini.

3.4 NFC čtečka PN532

NFC modul PN532 dokáže komunikovat pomocí I2C (Inter-Integrated Circuit), SPI (Serial Peripheral Interface), HSU (HIGH SPEED UART). Díky přepínačům na desce lze komunikační technologie zvolit.
Čtečka podporuje tyto typy karet:

- Mifare 1k, 4k, Ultralight, a DesFire karty,
- ISO/IEC 14443-4 karty, např. CD97BX, CD light, Desfire, P5CN072 (SMX),
- Innovision Jewel karty, např. IRT5001 karty,
- FeliCa karty, např. RCS 860 a RCS 854.

Čtečka také umožňuje komunikaci se zařízeními obsahující operační systém Android s podporou emulace karet.



Obr. 3.3: PN 532.

3.4.1 Ovládání PN532 skrze Arduino

Pro ovládání NFC modulu PN532 byla použita knihovna Adafruit-PN532. Je nutné definovat proměnné, do kterých je po přiložení NFC tagu automaticky zapsána hodnota. Tyto proměnné jsou například uidLength (obsahující velikost UID) a pole `uid[]` (zde je zapsáno samotné UID.)
Příklad pro jednoduché čtečky NFC tagů.

```
1 #include <Wire.h>
2 #include <SPI.h>
3 #include <Adafruit_PN532.h>
4
5 #define PN532_IRQ (2)
6 #define PN532_RESET (3)
7
```

```
8  Adafruit_PN532 nfc(PN532_IRQ, PN532_RESET);
9  void setup(void) {
10   Serial.begin(115200);
11   nfc.begin();
12   uint32_t versiondata = nfc.getFirmwareVersion();
13   if (! versiondata) {
14     Serial.print("Didn't find PN53x board");
15     while (1);
16   }
17   Serial.print("Found chip PN5");
18   Serial.println((versiondata>>24) & 0xFF, HEX);
19   Serial.print("Firmware ver. ");
20   Serial.print((versiondata>>16) & 0xFF, DEC);
21   Serial.print('.');
22   Serial.println((versiondata>>8) & 0xFF, DEC);
23   nfc.setPassiveActivationRetries(0xFF);
24   nfc.SAMConfig();
25
26   Serial.println("Waiting for an ISO14443A card");
27 }
28 void loop(void) {
29   boolean success;
30   uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };
31   uint8_t uidLength;
32   success = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A,
33    &uid[0], &uidLength);
34   if (success) {
35     Serial.println("Found a card!");
36     Serial.print("UID Length: ");
37     Serial.print(uidLength, DEC);Serial.println(" bytes");
38     Serial.print("UID Value: ");
39     for (uint8_t i=0; i < uidLength; i++)
40     {Serial.print(" 0x");
41       Serial.print(uid[i], HEX);}
42     Serial.println("");
43   delay(1000);}
44   else
45   {    Serial.println("Timed out waiting for a card");}
46 }
```

3.5 SPI (Serial Peripheral Interface)

Jedná se o sběrnici, která je velice jednoduchá na implementaci jak fyzicky tak programově, a proto byla použita jako hlavní komunikační sběrnice mezi platformou Arduino a čtečkou NFC tokenů. Umožňuje komunikaci mezi dvěma a více zařízeními. V této komunikaci pracuje jeden v režimu master a ostatní v režimu slave. Master generuje hodinový signal, který rozvádí do všech připojených zařízení a umožňuje tím kompletně synchronní komunikaci. Ke komunikace slouží čtyři vodiče a to SCK(Synchronous Clock), MISO (Master In, Slave Out), MOSI (Master Out, Slave In) a SS (Slave Select).

- SCK (hodinový kanál) generován masterem ,
- MISO (Datový kanál) přenaší data mezi masterem a slaves ,
- MOSI (Datový kanál) přenaší data mezi salves a masteres,
- SS (Slave Select) určuje, s kterým slaves komunikace probíhá.

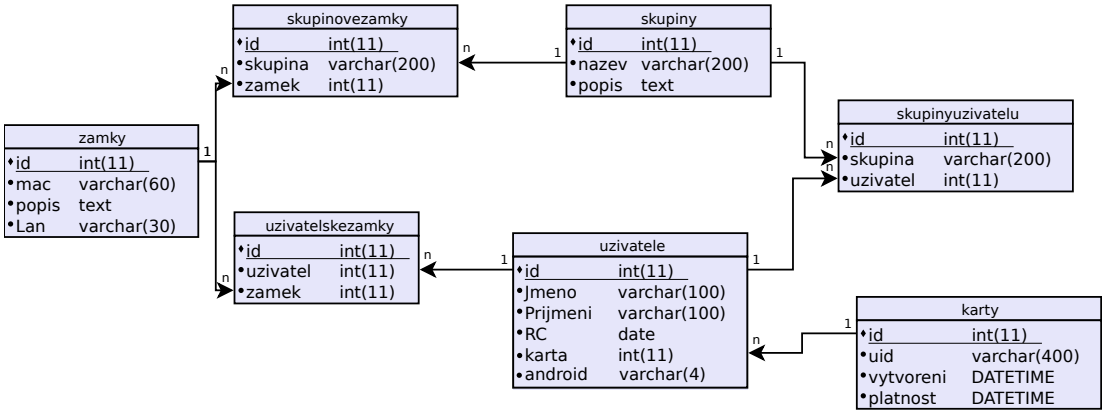
4 VYTVOŘENÉ APLIKACE

Vytvořená aplikace je rozdělena do tří funkčních bloků:

- databáze uživatelů,
- autentizační aplikace,
- uživatelské rozhraní.

4.1 Databáze uživatelů

Slouží jako úložiště o uživatelích, kartách, skupinách a zámcích. V této bakalářské práci je zvolena databáze MySQL. Celá databáze obsahuje tabulky zobrazené na Obr. 4.1.



Obr. 4.1: Diagram relací vytvořené databáze.

4.1.1 Tabulka uživatelů

Tato tabulka byla vytvořena k uchování informací o uživatelích. Patří sem **ID**, tento sloupec je generován automaticky při vytvoření uživatele a to inkrementační metodou. Číslo může dosahovat 11 řádů. **Jmeno** a **Prijmeni** jsou sloupce typu varchar s maximální délkou 100 znaků, vytvořené hlavně k jednoduchému vyčtení konkrétní osoby. Pokud je v databázi více osob se stejným jménem a příjmením, je zde k upřesnění **RC** typu date. **RC** je datum narození uživatele pro přesnou identifikaci. Dalším parametrem je **karta**, která má svůj cizí klíč svázaný s primárním klíčem **id** v tabulce karty. Sloupec **Karta** je typu int a může dosahovat 11 řádů. Je tedy relačně navázán na tabulku **karty** a pokud není přiřazena má hodnotu **NULL**. Jako poslední parametr je **android**, který má pouze 4 znaky, a to protože může nabývat třech hodnot: **YES**, **NO** a **WANT**.

- YES - Android zařízení má možnost přístupu,
- NO - android zařízení nemá možnost přístupu,
- WANT - android zařízení žádá o možnost přístupu.

4.1.2 Tabulka skupiny

Tato tabulka slouží k udělování hromadného oprávnění uživatelům. Například ve velkých společnostech obsahujících velký počet zaměstnanců. Tabulka obsahuje automaticky generované **id** typu int a počtem řádů 11, které se vytváří s vytvořením skupiny. Dále obsahuje **nazev**, který je typu varchar jeho maximální počet znaků je 200 a je identifikátorem skupiny. **Popis** typu text slouží k popsání skupiny.

4.1.3 Tabulka karty

Tabulka karty byla vytvořena jako seznam všech dostupných karet. Každá karta má také svoji platnost. Počáteční je při jejím vložení do systému a koncová rok od dne kdy byla přiřazena. Tyto údáje jsou ve sloupcích **vytvoreni** a **platnost** a parametry jsou typu datetime. Pro identifikaci karty byl vytvořen sloupec **uid**, ten je typu varchar a může dosahovat 400 znaků. Identifikace v databázi je určena hodnotou ve sloupci **id**, která je typu int a může dosahovat 11 řádů.

4.1.4 Tabulka zámky

Tato tabulka byla vytvořena pro identifikaci zámků otevírající jim přidělené dveře. Dveře jsou popsány ve sloupci **popis**, který je typu text. Byl zde také vytvořen sloupec s názvem **mac**, který je typu varchar a může obsahovat až 60 znaků udržujících fyzickou adresu příslušného ESP modulu. Dále je zde sloupec **lan**, který byl vytvořen jako držitel IP (Internet Protocol) adresy v LAN (Local Area Network) síti a je typu varchar. Může dosahovat až třiceti znaků. I zde byl vytvořen sloupec **id** typu int dosahující maximálně 11 řádů.

4.1.5 Tabulka uživatelských zámků

Jedná se o pomocnou tabulku pro udržení záznamů N:N. Obsahuje cizí klíče od id tabulek **uzivatele** a **zamky**. Dále obsahuje **id** záznamu, což je inkrementační identifikátor daného záznamu, který je typu int a může dosahovat 11 řádů. Tabulka obsahuje záznamy o tom, který uživatel má oprávnění k jakému zámku.

4.1.6 Tabulka skupinových zámků

Opět se jedná o pomocnou tabulka pro udržení záznamů N:N. Obsahuje zde cizí klíče a to **id** tabulky **zamky** a název tabulky **skupiny**. Dále obsahuje **id** záznamu což je inkrementační identifikátor daného záznamu, který je typu int a může dosahovat 11 řádků. Tabulka obsahuje záznamy o tom, které skupiny mají přístup k jakým zámkům.

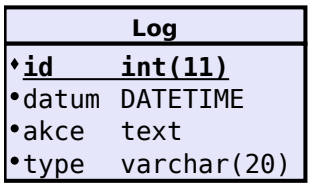
4.1.7 Tabulka skupiny uživatelů

Pomocná tabulka pro udržení záznamů N:N, která obsahuje cizí klíče a to **id** tabulky **uzivatele** a název tabulky **skupiny**. Dále obsahuje **id** záznamu, což je inkrementační identifikátor daného záznamu, který je typu int a může dosahovat 11 řádů. Tabulka obsahuje záznamy o tom, který uživatel patří do které skupiny (každý uživatel může patřit do více skupin).

4.1.8 Tabulka Log

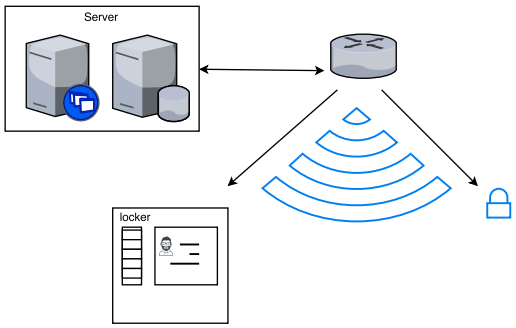
Je tabulka určená pro zaznamenávání aktivity v systému. Sloupec **datum** obsahuje datum a čas akce, proto je typu datetime. Sloupec **akce** je typu text a obsahuje popis provedené akce. Sloupec **type** definuje typ akce a je typu varchar. Má maximální počet znaků 20 a nabývá těchto hodnot:

- open - povolení přístupu uživateli,
- close - nepovoleni přístupu uživateli,
- change - změna v databází.



Obr. 4.2: Tabulka Log.

S vytvořenou databází komunikuje pouze serverová aplikace a Apache server, které jsou umístěné na stejném stroji. Jak lze vidět na diagramu 4.3



Obr. 4.3: Server diagram.

4.2 Návrh desky plošného spoje

Návrh desky plošného spoje byl rozdělen na dvě části a to z důvodu jak bezpečnostni tak možnosti rozšíření o další moduly. Jedna deska byla vyrobena pro umístění uvnitř zabezpečeného objektu a druhá k použití mimo zabezpečený objekt k umožnění přístupu dovnitř objektu. Vnitřní deska obsahuje obvod zajišťující bezdrátovou komunikaci se serverovou částí pomocí technologie WiFi. Dále obsahuje obvody zajišťující ovládání zámku tím umožnit osobám přístup do zabezpečeného objektu. Deska obsahuje rozhraní pro připojení napětí 12V, rozhraní pro připojení elektrického zámku a rozhraní pro připojení druhé desky plošného spoje. Tyto desky se připojují pomocí ethernetového kabelu. Ten byl zvolen z důvodu relativně malé velikosti a dostatečného počtu vodičů pro komunikaci všech prvků. Druhá deska obsahuje pouze komponenty nezbytné pro interakci s uživatelem jako je NFC modul PN532, piezo reproduktor nebo LED signalizující umožnění či zamítnutí přístupu.

4.2.1 DPS pro použití uvnitř zabezpečeného objektu

Hlavní komponentou tohoto plošného spoje je 8mi bitový processor Atmega328, ten se stará o obsluhu NFC čtečky, se kterou komunikuje pomocí SPI sběrnice. Jeho dalším úkolem je spínat elektronický zámek pomocí relé. Ke komunikaci se serverem je použit bezdrátový modul ESP8266, který je ovládán pomocí AT příkazů a slouží ke komunikaci se serverovou částí. Obvod pracuje se třemi úrovněmi napětí a to s 12V zdrojové napětí použíté pro otevírání zámku, které je převodníkem sníženo na 5V použité k napájení processoru ATMEGA328 a dále snížené na 3,3V pro napájení modulu ESP8266. Komunikace mezi moduly je uskutečněna skrze UART a jelikož moduly pracují v různých napěťových úrovních je nutné použít převodník napětí pro komunikaci skrze UART rozhraní. Pro potřeby programování processoru ATMEGA328 byla použita patice ICSP (In-Circuit Serial Programing) vyvedená na

DPS.

4.2.2 Program pro mikrokontroléru ATMEGA328

Pro snadnější komunikaci byl do processoru vypálen zavaděč Arduina a z tohoto důvodu byl kód psán v jazyce Wiring. Program se dělí na tři části:

NFC čtečka

První část se zabývá komunikací s NFC čtečkou PN532. Zde byla použita knihovna, která umožňuje po správném nastavení sestavit komunikaci typu bod-bod s Android zařízením a vyměňovat si data. Arduino pomocí čtečky zjistí, zda zařízení komunikuje v režimu bod-bod a obsahuje stejné AID. Pokud AID neobsahuje, nebo komunikace neprobíhá v režimu bod-bod, tak vezme jeho UID a dále jej zpracuje.

Komunikace se serverem

Komunikaci se serverem zajišťuje část obvodu obsahující WiFi modul ESP8266. S tím mikrokontrolér komunikuje pomocí hardwarového UART. Komunikace probíhá skrze AT příkazy a pomocí nich Arduino odesílá data získaná ze čtečky přímo do serverové aplikace. Protože se aplikace chová pouze jako server, komunikaci může vytvořit pouze zámek, který se na něj připojuje, protože přenos dat je omezen pouze na to spojení, ve kterém zámek odesílá informace o kartě nebo Android zařízení. Z tohoto důvodu nelze odeslat zámku zprávu o tom, že má otevřít jiné zařízení.

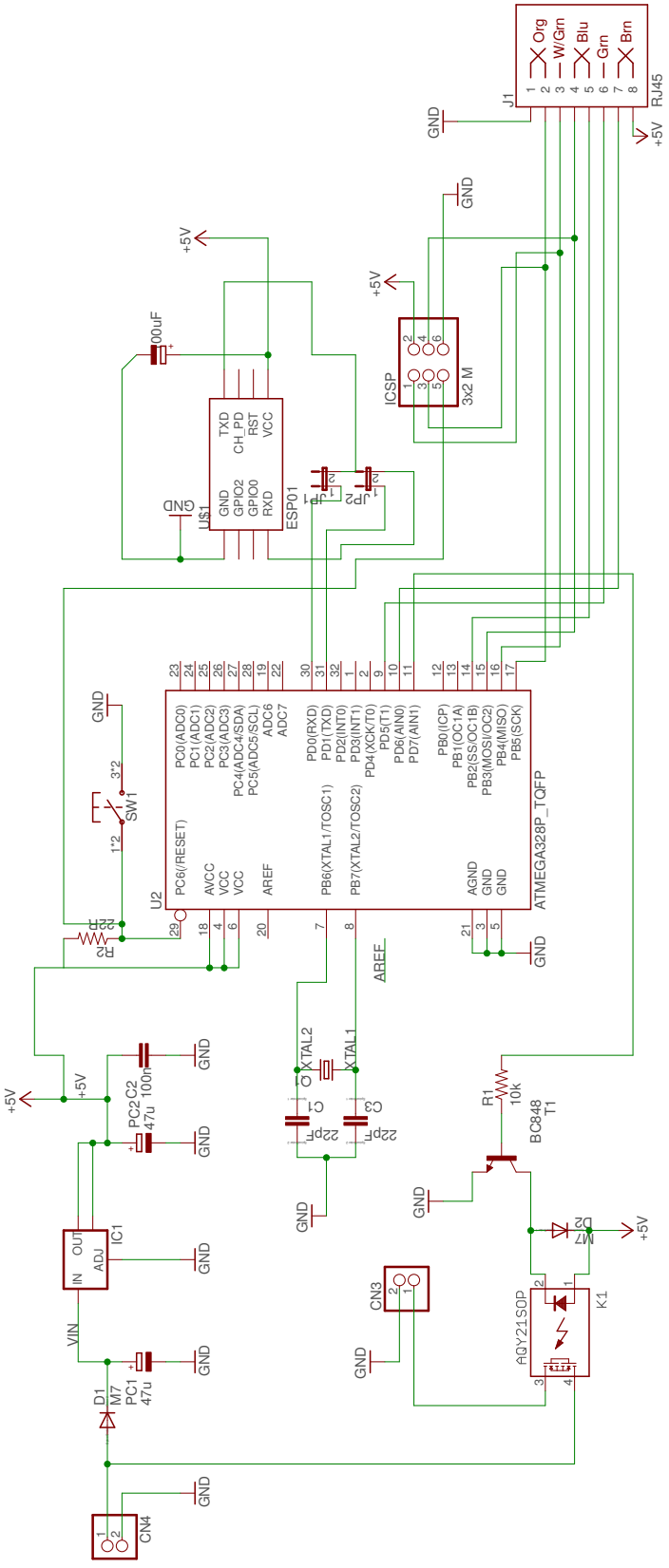
Spínání zámku

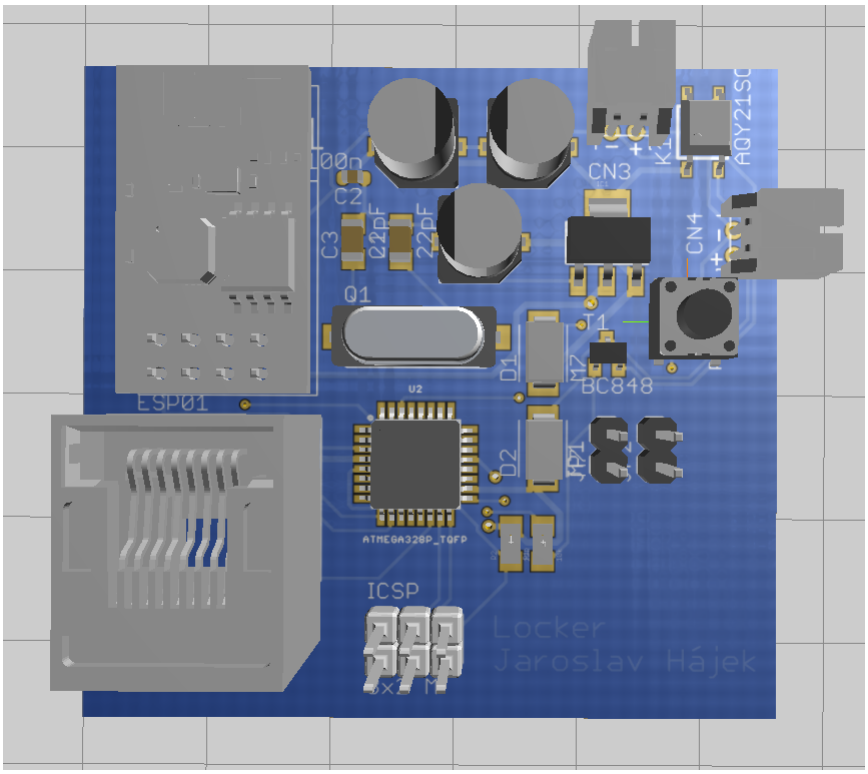
Protože je zámek napájen pomocí 12 V, tak je toto napájení použito i ke spínání samotnému elektronického zámku. Toho bylo docíleno pomocí relé, které je digitálním pinem spínáno skrze tranzistor.

4.2.3 Firmware v ESP8266

ESP8266 může obsahovat různé verze firmwaru jako je například NodeMCU, ve kterém se dá skriptovat v jazyce lua. Tato možnost byla v práci zvolena. Další možností je například jazyk MicroPython, ve které se dá psát v Pythonu, anebo v AT firmware. Ten je dobré použít pokud ESP používáme jako modul k jinému kontroléru. Nepoužijeme ho však v případě, že chceme programovat ESP samotné. Celkové schéma DPS je uvedeno na obrázku 4.4 a model DPS je vyobrazen na obrázku 4.5.

Obr. 4.4: Schéma vnitřního modulu.

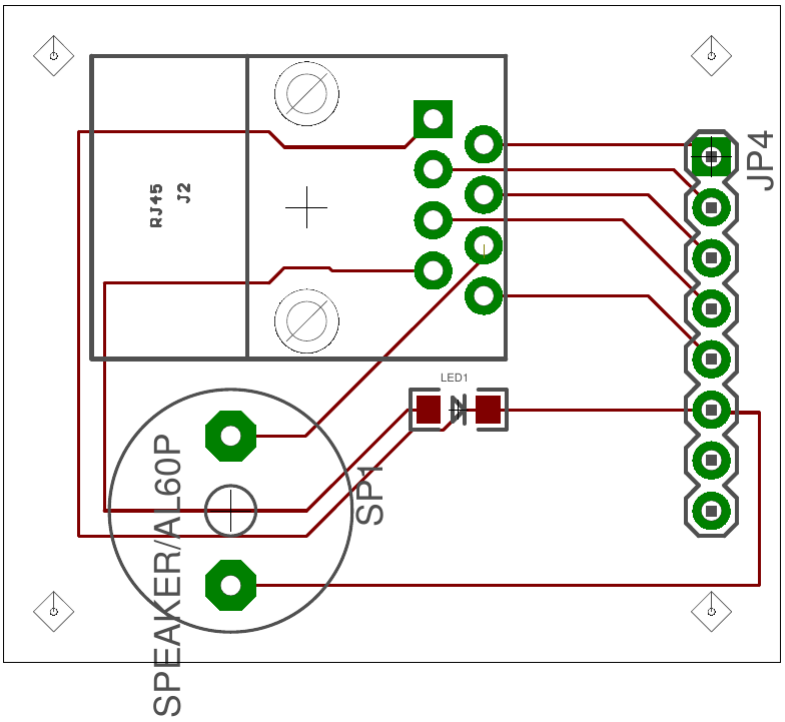




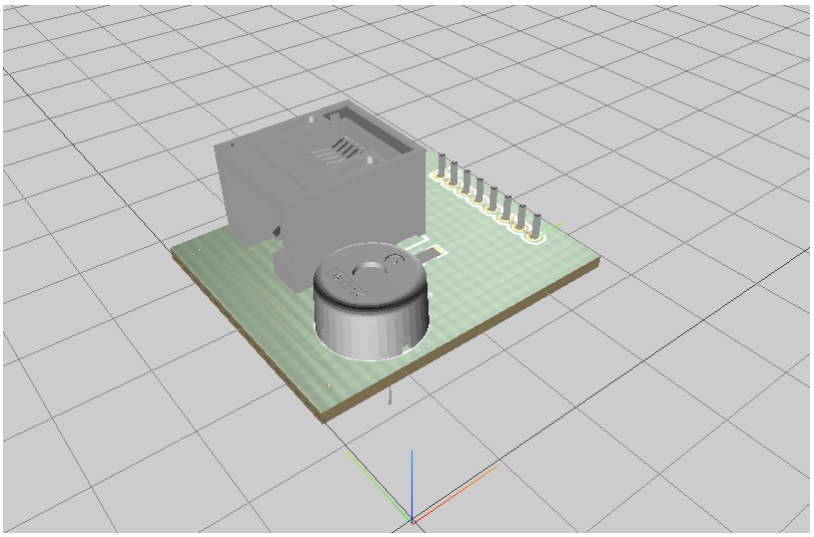
Obr. 4.5: DPS vnitřního modulu.

4.2.4 DPS umístěná mimo zabezpečený objekt

Pro authentizaci byla kvůlí bezpečnosti vyrobena i druhá deska plošného spoje, která na základě přístupové karty nebo Android zařízení uděluje přístup pro vstup do budovy. Tato DPS pro komunikaci s vnitřní DPS používá ethernetový kabel, který slouží pro přenos pomocí SPI. Díky tomu lze v budoucnu venkovní zařízení vyměnit například za čtečku otisku prstů. Schéma venkovní DPS je vyobrazeno na obrázku 4.6 a DPS na obrázku 4.7.



Obr. 4.6: Schéma venkovního modulu.



Obr. 4.7: DPS venkovního modulu.

4.3 Authentizer (serverová aplikace)

Tato aplikace byla napsána v jazyce Java a slouží jako prostředník mezi zámky a databází. Ke komunikaci používá transportní protokol TCP a naslouchá na portu 5631, čeká na příkaz **verify**. Tento příkaz odesílá WeMos D1 mini po přiložení karty s parametry mac adresa zámku a uid karty. Server tyto parametry ověří a odešle příkaz pro povolení či odmítnutí přístupu. Zároveň tyto akce zaznamenává do logu.

4.4 Locker (Webové rozhraní)

Webové rozhraní Locker je grafické rozhraní pro správu uživatelů, skupin a jejich přístupů. Slouží také pro správu zámků karet a jejich platností. Toto webové rozhraní je rozděleno na několik stránek a to na:

- Board,
- Uživatelé,
- Skupiny,
- Karty,
- Zámky,
- Log.

4.4.1 Board

Stránka Board slouží jako úvodní stránka webu, obsahuje výpis online zámků a výpis posledních povolení či zamezení přístupu k zámku.

4.4.2 Uživatelé

Na stránce uživatelé je vypsán seznam uživatelů, kde u každého uživatele lze měnit jeho oprávnění k zámkům či připojení karty k jeho osobě. Na každém řádku je tlačítko smazat sloužící pro smazání uživatele. Tlačítko nový zobrazí dialog pro vytvoření uživatele.

4.4.3 Skupiny

Stránka skupiny zobrazuje seznam skupin, kde nalezneme u každého uživatele tlačítko členové, zámky a tlačítko smazat. Tlačítko členové zobrazí členy této skupiny s možností přidání či odebrání uživatelů. Tlačítko zámky zobrazí seznam zámků, ke kterým má skupina oprávnění i zde je tlačítko přidat či odebrat.

4.4.4 Karty

Stránka karty obsahuje výpis seznamu karet s jejich uid, datumem přidání do systému a jejich platností. Pokud platnost vyprší zobrazí se tlačítko pro její prodloužení. Pomocí tlačítka nový lze do systému přidat novou kartu. Pokud je změněn zámek na stránce zámky jako administrativní, tak jej lze používat jako čtečku karet v systému Locker. Pokud je tedy zámek nastaven jako administrativní a je zvoleno přidat novou kartu, systém vyzve k přiložení nové karty.

4.4.5 Zámky

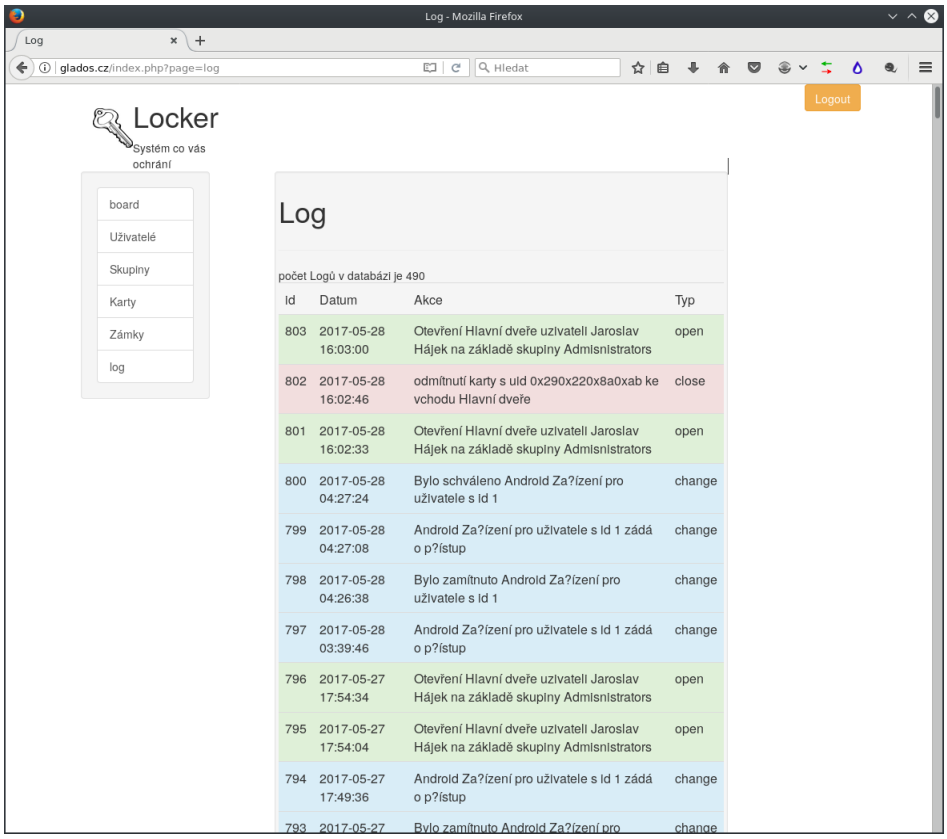
Stránka zámky obsahuje seznam všech zámku, jejich fyzickou adresu a popis. Pokud byl zámek v síti použit v posledních 5 minutách, je pole lan obsahující ip adresu zámku a tlačítko pro změnu zámku v administrativní či jeho vrácení do původního stavu. Každý zámek obsahuje tlačítko smazat pro jeho odstranění. Tlačítko nový zobrazí dialog pro přidání nového zámku.

4.4.6 Log

Stránka Log zobrazuje seznam veškeré aktivity s databází či přístupu a obsahuje čtyři druhy úrovní oznámení odlišené barvami:

- zelená - řádek se zobrazí zeleně pokud je záznam v logu typu open,
- červená - pokud je záznam typu close,
- modrá - pokud je záznam typu change,
- žlutá - pokud je záznam typu info.

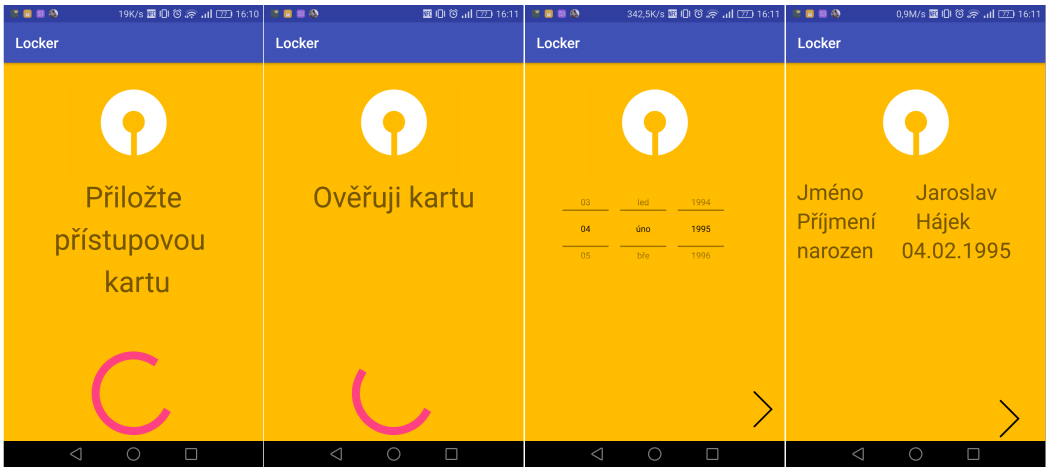
Na obrázku 4.8 je stránka zobrazující výpis logu.



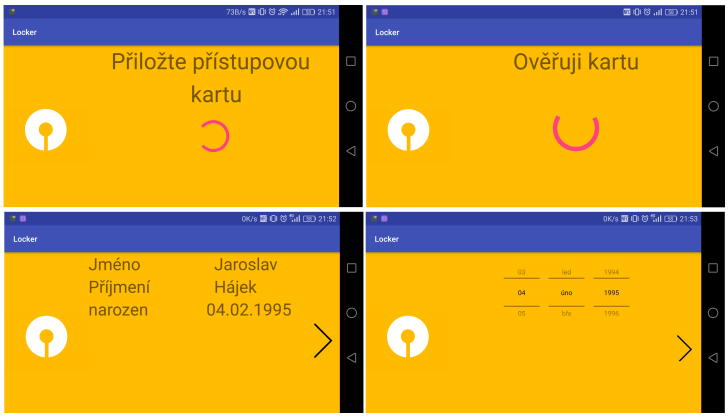
Obr. 4.8: Locker - Log.

4.5 Android Aplikace

Aplikace je napsána v prostředí Android Studio. Jako minimální verze systému Android, pro který je tato aplikace vyvinuta je Android 4.4 Kitkat. Tato verze byla zvolena z prostého důvodu, a to protože od verze Androidu 4.4 není potřeba k emulaci karty používat bezpečnostní prvek. V aplikaci je vytvořena pouze jedna aktivita `MainActivity.java`. Tato třída vytváří uživatelský účet, ve kterém je uložen řetězec, který je později odesílán NFC čtečce. Aby byl účet vytvořen je potřeba k zařízení přiložit kartu přiřazenou k Locker účtu. Po naskenování karty je zařízením odeslán požadavek na PHP server s předaným UID karty. Serverem je vracena jednoduchá odpověď ve tvaru `Jmeno;Příjmení;uid`. Po přijetí této odpovědi jsou uživateli zobrazeny údaje Jméno a Příjmení. Uživatel je po té vyzván k vložení data narození. Následně je odeslán serveru požadavek obsahující Jméno, Příjmení, datum narození. Server ověří datum narození podle Rodného čísla a odešle administrátorovi systému formulář ke schválení používaní Android zařízení jako virtuální karty pro přístup. Vzhled MainActivity je definován dvěmy rozloženími a to pro orientaci na výšku 4.9 a šířku 4.10



Obr. 4.9: Locker MainActivity.



Obr. 4.10: Locker MainActivity.

Služba `MyHostApduService.java` je služba, která umožňuje Android zařízení komunikovat s NFC čtečkou. Hlavní metodou této služby je `byte[] processCommandApdu(byte[] comandApdu)`. Před zahájením komunikace si Android zařízení ověří definované AID registrovaných služeb. V případě aplikace Locker se jedná o AID **F0050607080910**. Po shodě AID je zavolána metoda processCommandApdu, které předá commandApdu. Tato proměnná obsahuje příkaz odeslaný z NFC čtečky. V případě systému Locker se jedná o příkaz `auth`. Po odeslání příkazu čtečka čeká na řetězec odeslaný Android zařízením. Tato odpověď je převzata z Android účtu z proměnné hash. Řetězec je kombinací jména příjmení a uid. Při odeslání odpovědi vykreslí zařízení Logo Lockeru, které je uvedeno na obr. 4.11.

Služba `AuthenticatorService.java` je použita k vytváření účtu pro systém android. Důležitější je třída `CustomAuthenticator`, která definuje metody vyvolané systémovým nastavením jako je vytvoření účtu nebo změna vlastností. V souboru authenticator.xml je definováno tak, jak jsou v nastavení učtu prezentovány uživateli. Pokud se uživatel pokusí přidat více účtů do zařízení je mu v tomto kroku zabráněno. Nový účet lze do zařízení přidat až po odstranění předchozího uloženého účtu.

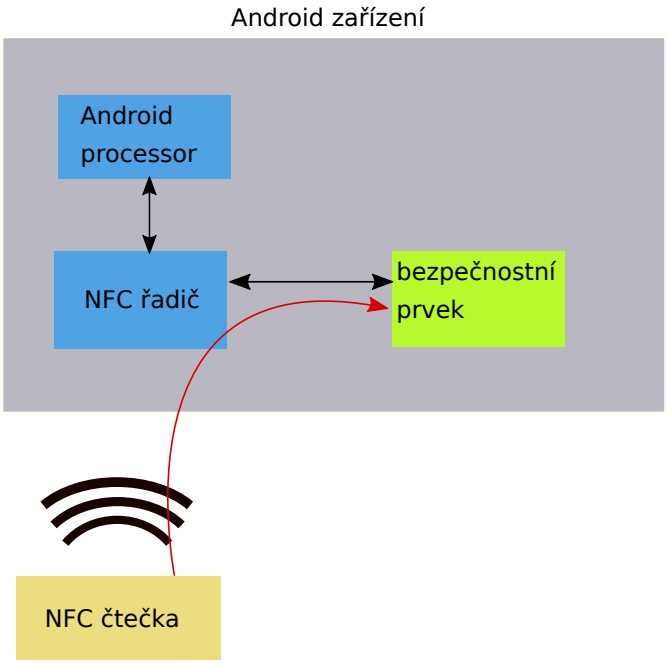
Obr. 4.11: Locker karta.

5 EMULACE KARET NA OPERAČNÍM SYSTÉMU ANDROID

Operační systém Android podporuje několik protokolů, které jsou využívány zejména v souvislosti s platebními transakcemi. Mnoho bezkontaktních karet tyto protokoly využívá pro bezkontaktní platební systémy. Tyto protokoly jsou také podporovány mnoha platebními terminály. To umožňuje postavit NFC řešení pro platby používající zařízení s operačním systémem Android.

5.1 Emulace karty využívající bezpečnostního prvku

Pokud je u emulace karty použit bezpečnostní prvek, karta je uložena v tomto bezpečnostním prvku. Pokud je zařízení přiloženo k terminálu NFC terminálu, tak NFC řadič v zařízení směřuje veškerou komunikaci přímo do bezpečnostního prvku. Jak lze vidět na obrázku 5.1. Protože bezpečnostní prvek komunikuje samostatně s NFC terminálem, nefiguruje zde Android aplikace. Pouze po dokončení přenosu si může aplikace vyžádat stav a informovat uživatele.

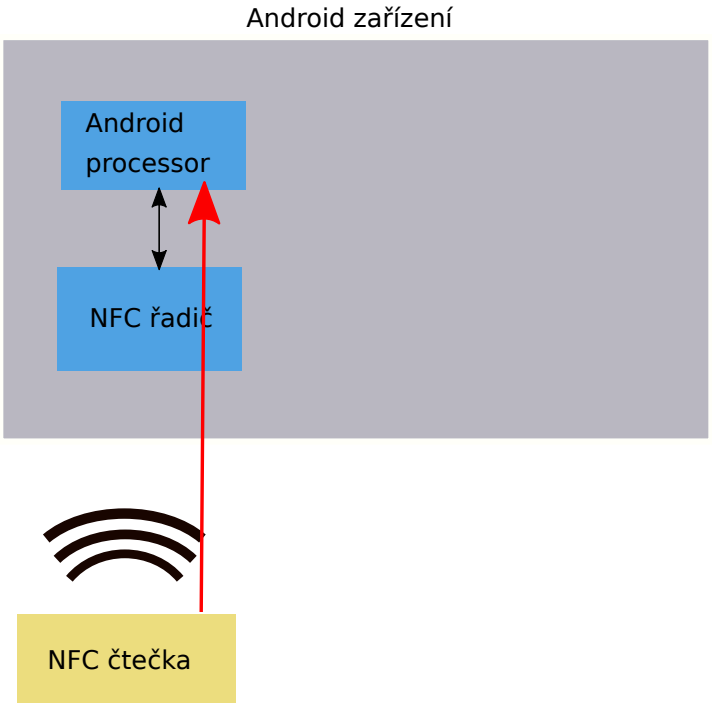


Obr. 5.1: Komunikace s bezpečnostním prvkem.

5.2 Emulace karty bez bezpečnostního prvku

Pokud je karta emulována bez bezpečnostního prvku, jsou data směrována přímo k Android aplikaci namísto směrování NFC komunikace k bezpečnostnímu prvku. Obrázek 5.2 znázorňuje jak tato komunikace probíhá.

Od systému Android 4.4 je podporovaná emulace karet založených na specifikaci NFC-Fóra ISO-DEP (založena na ISO/IEC 14443-4 [19]) a procesu aplikační procesorové datové jednotky definované specifikací ISO/IEC 7816-4 [20].



Obr. 5.2: Přímá komunikace s Aplikací.

5.3 Služby emulace karty

Architektura HCE (Host Card Emulation) je založena na komponentech android služeb známých jako "HCE services". Jedna z klíčových funkcí služeb je možnost běhu na pozadí bez jakékoli interakce uživatele. To je užitečné, například při obchodních platebních transakcí. Kdy není po uživateli požadováno spuštění speciální aplikace. Telefon vybere konkrétní službu, ta pokud není na pozadí již spuštěná se spustí a postará o transakci dat. Je zde i možnost o této skutečnosti informovat uživatele (pokud je to potřeba).

5.3.1 Výběr služby

Při inicializaci spojení Android zařízení potřebuje vědět, kterou ze služeb vybrat. Pro tento účel slouží standard ISO/IEC 7816-4 [20], který definuje výběr aplikace pomocí AID (Aplication ID). AID může obsahovat až 16 bajtů. Pokud jsou emulovány karty pro existující NFC infrastrukturu, tak AID, které čtečka hledá, jsou veřejně známy. Například AID platebních sítí, jako je Visa a MasterCard. Pokud chceme vytvořit novou infrastrukturu pro vytvořenou aplikaci, je nutné zaregistrovat nové AID. Registrační procedura je definovaná ve specifikaci ISO/IEC 7816-5 [21]. Je nutné zvolit vhodné AID, tak aby nedošlo ke kolizi s jinými identifikátory registrovaných služeb.

5.3.2 Kontrola podpory HCE

Před začátkem komunikace je nutné ověřit zda zařízení disponuje podporou funkce NFC HCE. K tomuto účelu slouží dvě metody `getSystemAvailableFeatures()` a `hasSystemFeature(String)`, jako argument druhé metody slouží řetězec `"FEATURE_NFC_HOST_CARD_EMULATION"`. V souboru manifest je nutné definovat, že aplikace využívá služeb HCE a zda jsou tyto služby potřebné k běhu aplikace. [22]

5.3.3 Implementace služby

Se systémem Android 4.4 byla vydána nová služba nazývaná `HostApduService`. Ta může být použita pro jednoduchou implementaci HCE. V prvním kroku je nutné založit třídu vycházející z rodičovské HostApduService, kterou bude nově vytvořená třída rozšiřovat. HostApduService definuje dvě abstraktní metody, které je třeba implementovat. Jsou to třídy:

- `public byte[] processCommandApdu(byte[] apdu, Bundle extras)`
- `onDeactivated(int reason)`.

```
1  public class MyHostApduService extends HostApduService {
2      @Override
3      public byte[] processCommandApdu(byte[] apdu, Bundle extras) {
4          ...
5      }
6      @Override
7      public void onDeactivated(int reason) {
8          ...
9      }
10 }
```

- **processCommandApdu**: tato metoda je zavolána vždy, když čtečka odešle APDU této službě. Zde je možnost odeslat odpověď a to návratovou hodnotou nebo pomocí metody `sendResponseApdu()`. Té je možno využít, pokud je nutné odpověď odeslat později.

5.3.4 AID registrace a deklarace service manifest

Služba musí být deklarována v manifestu, ale některé části musí být přidány do deklarace služby.

Nejprve je nutné definovat, která ze služeb implementuje HCE rozhraní služby `HostApduService`. Deklarace služby musí obsahovat `intent filter` pro `SERVICE_INTERFACE` akce. Dále je potřeba nastavit platformě, které AID skupiny se mají služby dotazovat. Je tedy potřeba vložit `<meta-data>` tag ukazující na XML (Extensible Markup Language) soubor s dodatečnými informacemi o HCE službě. Nakonec je přidáno oprávnění pro přístup k NFC zařízení. Jde o oprávnění `android.permission.BIND_NFC_SERVICE`). Zde je příklad deklarace služby v souboru manifest.

```
1 <service android:name=".MyHostApduService" android:exported="true"
2 android:permission="android.permission.BIND_NFC_SERVICE">
3 <intent-filter>
4 <action android:name="
5 android.nfc.cardemulation.action.HOST_APDU_SERVICE"/>
6 </intent-filter>
7 <meta-data android:name="android.nfc.cardemulation.host_apdu_service"
8 android:resource="@xml/apduservice"/>
9 </service>
```

5.4 Android Aktivita

Aktivita je základní prvek pro vykreslování grafických komponent na obrazovku displeje. Jako příklad Aktivity lze uvést například menu aplikace, ve kterém umístěny prvky pro přesun do jiné aktivity. Přepnutí do aktivity přitom není omezeno jen v rámci aplikace, lze se tedy přepínat i do aktivity aplikace jiné. Pokud je nutné vyvolat aplikaci pro vytáčení, nemusíme tuto aktivitu vytvářet znovu, ale pouze se přepne na aplikaci pro telefonování.

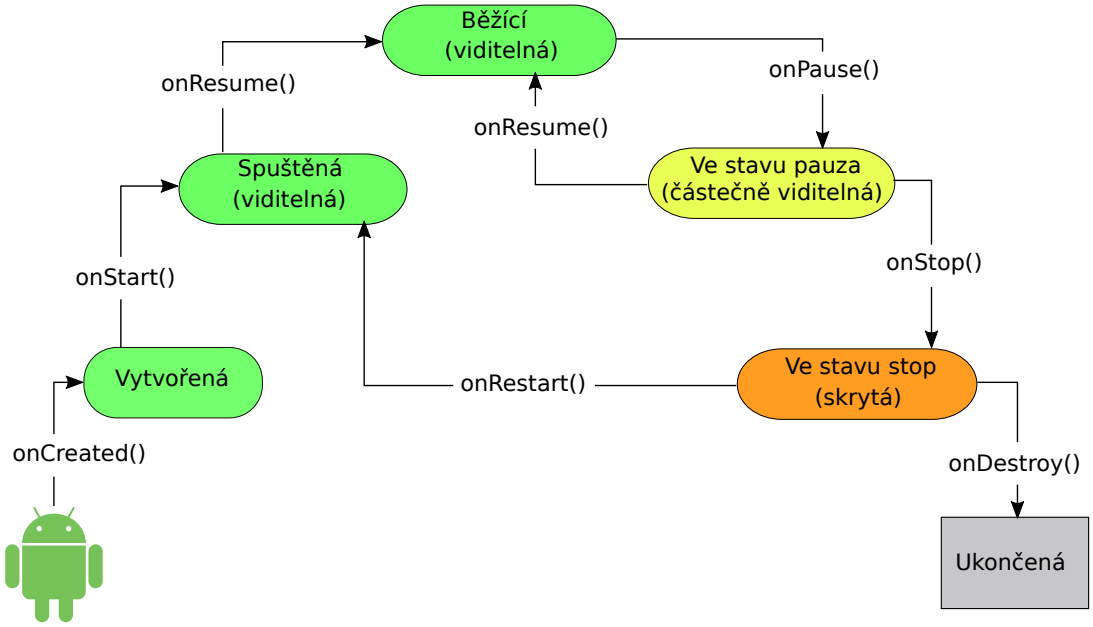
5.4.1 Životní cyklus aktivity

V zařízeních se systémem Android může docházet k situacím, které jsou vytvářeny buď interakcí uživatele nebo systémem samotným. Jednou z uživatelských interakcí může být minimalizování aplikace ze systémových, je to například příchozí hovor. Z těchto důvodů není vždy jasné jak dlouho aktivita poběží. Proto vznikla sada metod, které se spouští na základě stavu aplikace. Každá aktivita má čtyři základní stavy:

- Běží - v tomto stavu je aplikace, která se úspěšně spustila a je uživateli zobrazena v popředí.
- Pauza - v tomto stavu je aktivita pokud je vidět v pozadí a překrývá jí dialog, nebo aktivita jiná jako je například příchozí hovor. V tomto stavu nelze s aktivitou nijak pracovat.
- Zastavená - je aktivita tehdy pokud není uživateli viditelná a nemá k ní přístup, tato aktivita ještě není ukončená. Je to například aplikace, která je minimalizována domovským tlačítkem.
- Ukončená - je aplikace tehdy pokud už není v seznamu minimalizovaných aplikací je tedy úplně ukončená a nejde se k ní vrátit jinak než opětovným spuštěním.

5.4.2 Metody průběhu aplikace

Tyto metody jsou spouštěny při přechodu aplikace mezi základními stavy. Přechody mezi těmito stavy jsou zobrazeny na diagramu 5.3.



Obr. 5.3: Životní cyklus Aktivity.

5.5 Android Manifest

Android aplikace je možné vytvářet ze čtyř hlavních komponent:

- Aktivity - grafické rozhraní aplikace.
- Services - služba která nemá grafické rozhraní a běží dlouhodobě na pozadí.
- Content providers - možnost jak sdílet data z aplikace (kontakty, sms)
- Broadcast Intent Receivers - naslouchá zda nějaká aplikace nechce například přehrát video a pokud to tato aplikace umí, nabídne se pro jeho přehrání.

Všechny tyto prvky musí být deklarovány v souboru **AndroidManifest.xml** díky tomu systém ví, co a jak volat a jakým způsobem se aplikace chová ke svému okolí. Další věc, která je definovaná v AndroidManifest.xml jsou oprávnění aplikace. Ty slouží k tomu aby byl uživatel předem informován o tom, jaké senzory a data může aplikace využívat.

6 ZÁVĚR

Cílem této bakalářské práce bylo vytvoření univerzální platformy pro autentizaci uživatelů pomocí předmětů. Všechny body zadání byly splněny a vytvořená aplikace umožňuje autentizaci uživatelů skrze čipové karty a mobilní zařízení využívající technologii NFC.

Původní návrh počítal s aplikací přístupnou pouze z lokálního serveru založenou na technologii NFC. Z důvodu větší univerzálnosti byla nakonec vytvořena webová aplikace založená na technologii PHP. Výsledná platforma je rozdělena do čtyř částí, první se skládá z NFC čtečky a mikrokontroléru ATmega 328p společně s WiFi modulem pro komunikaci se serverovou částí. Server obsahuje dva oddělené moduly, první je napsán v jazyce Java a zajišťuje autentizaci uživatelů oproti databázi. Aplikace obsahuje dva komunikační porty, první je nezabezpečený a může být použit pro autentizaci uživatelů. Druhý poskytuje šifrovanou komunikaci a kromě autentizace umožňuje správu uživatelských účtů. Třetí částí je již zmíněné uživatelské rozhraní umožňující přehlednou správu autentizační platformy. Čtvrtá část obsahuje mobilní aplikaci pro platformu Android umožňující autentizaci na základě vestavěného NFC modulu s podporou emulace hostitelské karty.

Hlavním přínosem práce bylo zlepšení přístupových metod do objektů a budov pomocí technologie NFC implementované v přístupové kartě nebo v zařízení se systémem Android. Tato metoda zjednoduší autentizaci a autorizaci jednotlivých osob či skupin. Díky použití databáze s logováním událostí je zvýšena bezpečnost a správce systému má dále přehled o všech změnách v systému či případných pokusech o průniku do něj. Vzhledem k tomu že aplikace využívá vlastní otevřené programátorské rozhraní (API) lze jí implementovat do jakéhokoliv řešení. Díky modulárnosti systému, lze aplikaci rozšířit o elementy zvyšující zabezpečení systému. V případě čtečky to může být dodatečná klávesnice umožňující zadat heslo pro vstup. U mobilního telefonu to může být dodatečné potvrzení otiskem prstu či oční duhovky.

LITERATURA

[1] BURDA, Karel. *Zabezpečovací systémy* Vysoké učení technické v Brně Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací Purkyňova 118, 612 00 Brno: elektronicky, 2012, 96 - 97 [cit. 11. 12. 2016]. ISBN 78-80-214-4441-6. Dostupné z URL: <https://www.vutbr.cz/www_base/priloha.php?dpid=68532>.

[2] *Arduino Dokumentace* . elektronicky, 2012 . [online]. [cit. 11. 12. 2016]. Dostupné z URL: <http://docs.uart.cz/docs/io-piny/>.

[3] *Moderní způsoby programování mikrokontroléru* . Brno: Vysoké učení technické v Brně. Fakulta strojního inženýrství, 2015. [online]. [cit. 11. 12. 2016]. Dostupné z URL: <https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/41209/BP_Medla_152895.pdf>.

[4] *Raspberry Pi* In: Wikipedia: the free encyclopedia . San Francisco (CA): Wikimedia Foundation, 2001. [online]. [cit. 11. 12. 2016]. Dostupné z URL: <https://cs.wikipedia.org/wiki/Raspberry_Pi>.

[5] *NFC Forum* [online]. [cit. 11. 12. 2016]. Dostupné z URL: <http://nfc-forum.org/resources/what-are-the-operating-modes-of-nfc-devices/>.

[6] *NFC Forum* [online]. [cit. 11. 12. 2016]. Dostupné z URL: <http://nfc-forum.org/newsroom/nfc-forum-issues-specifications-for-four-tag-types/>.

[7] *NDEF Format* [online]. [cit. 11. 12. 2016]. Dostupné z URL: <https://learn.adafruit.com/adafruit-pn532-rfid-nfc/ndef>.

[8] *Přístupové terminály* [online]. [cit. 15. 10. 2016]. Dostupné z URL: <http://www.z-ware.cz/?36-pristupove-terminaly>.

[9] *Přístupové systémy* [online]. [cit. 15. 10. 2016]. Dostupné z URL: <http://www.technopark.cz/pristupove-systemy>.

[10] *Přístupové systémy* [online]. [cit. monitoring 15. 10. 2016]. Dostupné z URL: <http://www.elektroinstalace.cz/cz/obory-cinnosti/pristupove-systemy>.

[11] *Co je to NFC a co umí?* [online]. [cit. monitoring 15. 10. 2016]. Dostupné z URL: <https://nearfield.cz/co-je-nfc>.

[12] *Co je RFID* [online]. [cit. monitoring 15. 10. 2016]. Dostupné z URL: <http://www.rfidportal.cz/index.php?page=rfid_obecne>.

[13] *Arduino* [online]. [cit. 15. 10. 2016]. Dostupné z URL: <http://arduino.cc>.

[14] *Arduino Shop* [online]. [cit. 15. 10. 2016]. Dostupné z URL: <http://arduino-shop.cz>.

[15] RFC2046. *Multipurpose Internet Mail Extensions: (MIME) Part Two: Media Types.* [online].RFC Editor, 1996. [cit. 05. 03. 2017]. Dostupné z URL: <https://tools.ietf.org/pdf/rfc2046.pdf>.

[16] RFC3986. *Uniform Resource Identifier (URI): Generic Syntax* [online].RFC Editor, 1996. [cit. 05. 03. 2017]. Dostupné z URL: <https://tools.ietf.org/pdf/rfc3986.pdf>.

[17] COSKUN, Vedat., Kerem. OK a Busra. OZDENIZCI. *Near field communication: from theory to practice.* 1. Hoboken, NJ: Wiley, 2012. [cit. 05. 03. 2017]. ISBN 9781119971092.

[18] ROLAND, Michael. Software card emulation in NFC-enabled mobile phones: great advantage or security nightmare. In: *Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use.* [online]. 2012. p. 1-6. [cit. 05. 03. 2017]. Dostupné z URL: <https://pdfs.semanticscholar.org/f001/2b5311f65b4b2ebce21666842606ae89074d.pdf>.

[19] Identification cards — Contactless integrated circuit cards — Proximity cards — Part 4: Transmission protocol. *ISO/IEC 14443-4.* [online]. ISO/IEC JTC 1/SC 17, 3, 2016-06, 35.240.15 [cit. 05. 03. 2017]. Dostupné z URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-4:ed-3:v1:en>.

[20] Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange *ISO/IEC 7816-4.* [online]. ISO/IEC JTC 1/SC 17, 3, 2013-04, 35.240.15 [cit. 05. 03. 2017]. Dostupné z URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-4:ed-3:v1:en>.

[21] Identification cards — Integrated circuit cards — Part 5: Registration of application providers *ISO/IEC 7816-5.* [online]. ISO/IEC JTC 1/SC 17, 2, 2004-12, 35.240.15 [cit. 05. 03. 2017]. Dostupné z URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-5:ed-2:v1:en>.

[22] MACLEAN, Dave, Satya KOMATINENI a Grant ALLEN. *Pro Android 5.*[cit. 05. 03. 2017]. [Fifth edition]. ISBN 978-1-4302-4680-0.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

FTDI Future Technology Devices International

HSU High Speed Uart

IDE Integrované vývojové prostředí – Integrated Development Environment

IL délka identifikátoru – ID Length

I2C Inter-Integrated Circuit

LLCP Logical Link Control Protocol

MB Začátek zprávy – Message Begin

ME Konec zprávy – Message End

NDEF NFC Data Exchange Format

NFC Near Field Communication

OSI Open Interconnection Reference

RFID Radio Frequency Identification

SCL hodinový signál – Synchronous Clock

SDA datový kanál – Synchronous Data

SIM subscriber identify module

SPI Serial Peripheral Interface

SR krátký záznam – Short Record

TCP Transmission Control Protocol

TNF typ formátu – Type Name Format

UDP User Datagram Protocol

URL Uniform Resource Locator

HCE Host Card Emulation

SD Secure Digital

PICC Proximity Integrated Circuit Card

PCD Proximity Coupling Device

REQ Request Command

ATQA Answer To Request

APDU Application Processing Data Unit

UART Universal Asynchronous Receiver/Transmitter

USB Universal Serial Bus

ARM Acron RISC Machine

MySQL My Structured Query Language

SSID Service Set Identifier

SCK Synchronous Clock

MISO Master In, Slave Out

MOSI Master Out Slave In

SS Slave Select

IP Internet Protocol

LAN Local Area Network

ICSP In-Circuit Serial Programing

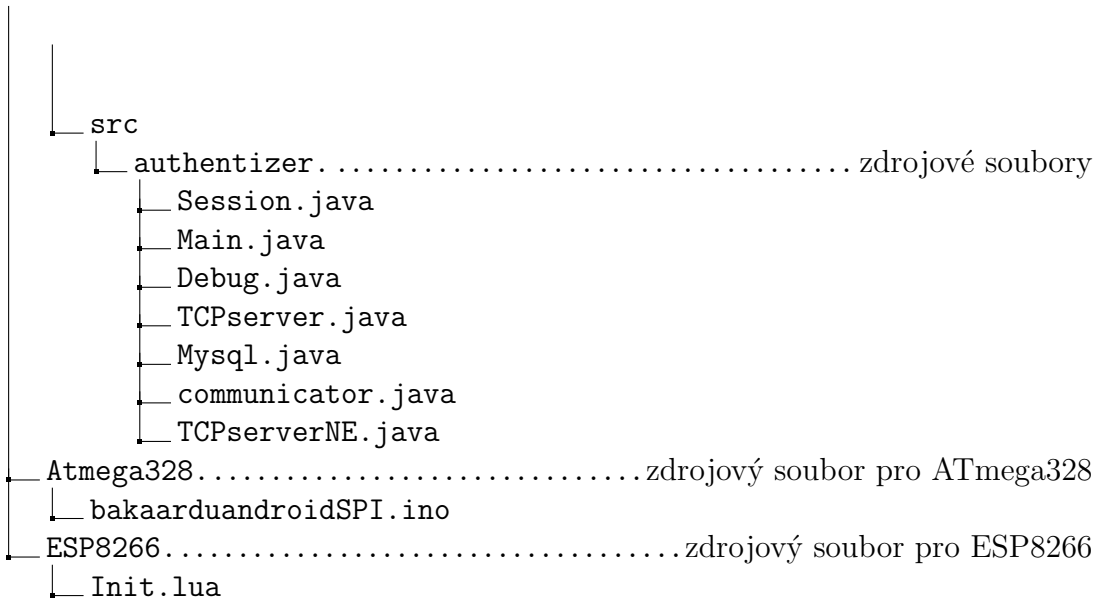
SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO CD

- / — Kořenový Adresář CD
  - WEB — Webová aplikace
    - config.php — soubor obsahující konfiguraci
    - index.php — hlavní soubor
    - install.php — instalační soubor
    - login.php — přihlašovací soubor
    - logout.php — odhlašovací soubor
    - api — složka obsahující soubory komunikující mimo web
      - android.php — soubor ověřující identitu Android uživatele
    - css — složka obsahující styly
      - bootstrap.min.css
      - klic.png
    - dialogy — složka obsahující dialogy komunikující se skripty
      - AddCard.php
      - AddGroup.php
      - AddLock.php
      - AddLockToGroup.php
      - AddLockToUser.php
      - AddUser.php
      - AddUserToGroup.php
      - CardToUser.php
    - js — JavaScriptové soubory
      - bootstrap.min.js
      - Chart.js
      - jquery-3.2.1.min.js
    - scripty — hlavní skripty vracející Json formát
      - AddCard.php
      - AddGroupUser.php
      - AddUser.php
      - ctecka.php
      - UpdateExpiration.php
      - AddGroupLock.php
      - AddLock.php
      - AndroidDevice.php
      - DELETE.php
      - UpdateUserCard.php
      - AddGroup.php
      - AddUserLock.php
      - CteckaInit.php
      - ODEBRAT.php
    - stránky — Stránky načítající se do těla webu
      - board.php
      - karty.php
      - log.php

- skupiny.php
- uzivatele.php
- zamky.php

- Android Aplikace. ..... Aplikace pro Android
  - AndroidManifest.xml
  - java
    - cz
      - jaroslavhajek
        - hcelocker. ..... zdrojové soubory
          - AuthenticatorService.java
          - DatePickerFragment.java
          - MainActivity.java
          - Poster.java
          - CustomAuthenticator.java
          - karta.java
          - MyHostApduService.java
          - SimpleScannerActivity.java
  - res. ..... zdrojové soubory (obrázky)
    - drawable
      - dialoglocker.xml
      - dialoglocker2.xml
      - ikona.xml
      - imglocker.png
      - logot.png
      - sipka.xml
    - layout. ..... rozvržení aplikace
      - activity-main.xml
      - content-simple-scanner.xml
      - hcedialog.xml
      - activity-simple-scanner.xml
      - date-dialog.xml
      - ldialog.xml
    - layout-land
      - activity-main.xml
    - values. ..... soubory hodnot
      - attrs.xml
      - colors.xml
      - dimens.xml
      - strings.xml
      - styles.xml
    - xml
      - apdu.xml
      - authenticator.xml
- authentizer. ..... Java serverová aplikace
  - extlibs
    - mysql-connector-java-5.1.38-bin.jar


src
authentizer
zdrojové soubory
Session.java
Main.java
Debug.java
TCPserver.java
Mysql.java
communicator.java
TCPserverNE.java
Atmega328
zdrojový soubor pro ATmega328
bakaarduandroidSPI.ino
ESP8266
zdrojový soubor pro ESP8266
Init.lua